Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) Method of authentication, wherein a client requests a file from a server, whereby the client and the server share a ~~common~~ secret value and thereby belong to an accepted group, comprising the step of:

the client forms a first message including

a filename,

a nonce which is associated with the ~~given~~ filename,

a first hash value according to a first hash function formed from the filename and the secret value.

2. (Previously Presented) Method according to claim 1, further comprising the step of the server extracting

the filename of a received first message,

extracting the first hash value,

forming a value of the received filename and the secret value,

forming a second hash value according to the first hash function formed from the value of the filename and the secret value,

comparing the first hash value with the second hash value and if the values are the same, establishing that the first message stems from a client belonging to the accepted group, otherwise establishing that the client does not belong to the accepted group.

3. (Previously Presented) Method according to claim 1, wherein the server responds to the request from the client by forming a second message including

a file corresponding to the requested filename,

the received nonce which is associated with the given filename,

a third hash value according to a second hash function formed from the value of the received nonce and the secret value.

4. (Previously Presented) Method according to claim 3, further comprising the step of the client

extracting the file of the received second message,

extracting the third hash value from the second message,

forming a value of the nonce associated with the filename and the secret value,

forming a fourth hash value according to the second hash function formed from the value of the nonce associated with the requested filename and the secret value,

comparing the third hash value with the fourth hash value and if the values are the same, establishing that the second message stems from a server belonging to the accepted group, otherwise establishing that the server does not belong to the accepted group.

5. (Previously Presented) Method according to claim 3, wherein the first hash function is the same as the second hash function.

6. (Previously Presented) Method according to claim 1, the inputs to said first hash function are concatenated.

7. (Currently amended) A method of authentication, comprising:

a client ~~Client~~ sharing a ~~common~~ secret value with a server, the client and the server thereby belonging to an accepted group, whereby

the client forms a first message comprising

a filename,

a nonce which is associated with the ~~given~~ filename,

a first hash value according to a first hash function formed from the values of the filename and the secret value, and whereby

the client receives a second message from the server, the client

extracting a file of the received second message,

extracting a third hash value from the second message,

forming a value of the nonce and the secret value,

forming a fourth hash value according to a second hash function formed from the value of the nonce associated with the requested filename and the secret value,

comparing the third hash value with the fourth hash value and if the values are the same establishing that the second message stems from a server belonging to the accepted group, and if otherwise, establishing that the server does not belong to the accepted group.

8. (Currently amended) A method of authentication, comprising:

a server ~~Server~~ sharing a ~~common~~ secret value with a client, the client and the server thereby belonging to an accepted group, whereby the server receives a first message from the client, the server

extracting [[the]] a filename and a nonce associated with the filename from the received first message,

extracting a first hash value from the received first message,

forming a value of the received filename and the secret value,

forming a second hash value according to the first hash function formed from the value of the filename and the secret value,

comparing the first hash value with the second hash value and if the values are the same establishing that the first message stems from a client belonging to the accepted group, otherwise establishing that the client does not belong to the accepted group.

9. (Currently amended) The method ~~Server~~ according to claim 8, wherein the server responds by sending a second message comprising

a file corresponding to the requested filename,

a third hash value according to a second hash function formed from the value of the received nonce associated with the filename and the secret value.